EO/US
PCT/EP99/04438

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing: 06 January 2000 (06.01.00)	
International application No.: PCT/EP99/04438	Applicant's or agent's file reference: P98033WO.1P
International filing date: 25 June 1999 (25.06.99)	Priority date: 26 June 1998 (26.06.98)
Applicant: POSEGGA, Joachim et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

10 November 1999 (10.11.99)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer: J. Zahra Telephone No.: (41-22) 338.83.38

Form PCT/IB/331 (July 1992)

3031325

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

DEUTSCHE TELEKOM AG
Rechtsabteilung (Patente) PA1
D-64307 Darmstadt
ALLEMAGNE

Date of mailing (day/month/year)
02 December 1999 (02.12.99)

Applicant's or agent's file reference
P98033WO.1P

IMPORTANT NOTIFICATION

International application No.
PCT/EP99/04438

International filing date (day/month/year)
25 June 1999 (25.06.99)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [ ] the agent [X] the common representative

Name and Address
DEUTSCHE TELEKOM AG
Technologiezentrum
Patentabteilung EK03
D-64307 Darmstadt
Germany

State of Nationality:
State of Residence:
Telephone No.: +49(61 51) 83-58 40
Facsimile No.: +49(61 51) 83-58 43
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address
DEUTSCHE TELEKOM AG
Rechtsabteilung (Patente) PA1
D-64307 Darmstadt
Germany

State of Nationality:
State of Residence:
Telephone No.: +49(61 51) 83-58 40
Facsimile No.: +49(61 51) 83-58 43
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
F. Baechler

Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994)

002986481

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International Reference PCT/EP99/04438

I. Basis of the report

1. This report has been prepared on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments):*

the Specification, pages 1-12 as originally filed

the Claims, nos. 1 as originally filed

V. Substantiated determination according to Article 35(2) with respect to novelty, inventive activity and industrial applicability; documents and clarifications in support of this determination

1. DETERMINATION

Novelty		Claims 1	YES
		Claims	NO
Inventive Activity	Claims 1		YES
		Claims	NO
Industrial Applicability	Claims 1		YES
		Claims	NO

2. DOCUMENTS AND CLARIFICATIONS

See enclosure.

VII. Specific Shortcomings of the International Application

It was determined that the International Application has the following shortcomings with regard to form or

EL594609247US

content:

see enclosure

With respect to Point V

Substantiated determination according to Article 35(2) with respect to novelty, inventive activity and industrial applicability; documents and clarifications in support of this determination

1. Reference is made to the following document:

D1: EP-A-0 685 792

2. The object of the present invention is to provide a method for checking Java byte code programs to check for safety properties in accordance with the principle of byte code verification, to ensure greater safety in executing such Java byte code programs.

This objective is achieved in accordance with the present invention in that the Java byte code program is transferred to a model checker, and the latter formally checks to determine whether the program fulfills certain safety properties. To make this possible, first the generally infinite state space of the Java byte code program must be mapped onto another suitable system having a finite number of states that the model checker is able to work with. This is accomplished in that all information, which is not needed, is rejected to determine whether the original byte code program is acceptable. This is done by replacing the concrete data values of the Java byte code program by abstract type information. The resulting state transition system thus possesses a finite quantity of states and can be processed by a model checker.

The subject matter of the present invention is distinguished from the teaching of document D1 in that the problem definition with respect to the safety of Java

byte code programs is neither identified in D1 nor is reference to a possible solution to the problem definition made in D1. Although the teaching of document D1 does, in fact, generally identify the problem definition of formally verifying systems on the basis of a model checker, and discloses an algorithm for reducing the state space of such systems to be verified, no reference is made as to how the algorithm described in D1 can be applied in the specific case to the verification of safety properties of Java byte code programs. Above all, no indication is given of being able to reduce the state space of Java byte code programs by replacing the specific data values by abstract type information.

Thus, the present International Application fulfills the requirements of Article 33(2) and (3) PCT with respect to novelty and inventive activity.

With respect to Point VII

Specific shortcomings of the International Application

1. In contradiction to the requirement of regulation 5.1 a) ii) PCT, neither the relevant related art disclosed in document D1 nor this document is provided in the Specification.

2. The independent Claim 1 is, in fact, formulated in the two-part form; however, all features except for "wobei alle nicht für die Zulässigkeit ... welche in einen Modelchecker eingegeben werden" [all information not needed for the acceptability ... which is input into a model checker] are incorrectly specified in the characterizing part, since they were disclosed in document D1 (regulation 6.3 b) PCT).

3. The following typographical errors in the International Application should be corrected:

(a) In Claim 1, line 12, "Zustandsübergangssystem" [state transition system] should be corrected to read "Zustandsübergangssystem" [state transition system]. **[Translator's note: there is no difference between the two terms here.]**

(b) In Claim 1, line 20, "ob ob" [whether whether] should be corrected to read "ob" [whether].

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :		(11) Internationale Veröffentlichungsnummer: **WO 00/00890**
G06F 11/00	**A1**	(43) Internationales Veröffentlichungsdatum: 6. Januar 2000 (06.01.00)

(21) Internationales Aktenzeichen: PCT/EP99/04438

(22) Internationales Anmeldedatum: 25. Juni 1999 (25.06.99)

(30) Prioritätsdaten:
198 30 015.8 26. Juni 1998 (26.06.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: POSEGGA, Joachim [DE/DE]; Eichelbergweg 16A, D–76646 Bruchsal (DE). VOGT, Harald [DE/DE]; Liebfrauenstrasse 5, D–64289 Darmstadt (DE).

(74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Rechtsabteilung (Patente) PA1, D–64307 Darmstadt (DE).

(81) Bestimmungsstaaten: US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD FOR CHECKING JAVA BYTE CODE PROGRAMMES FOR SECURITY CHARACTERISTICS

(54) Bezeichnung: VERFAHREN ZUR PRÜFUNG VON JAVA–BYTECODE–PROGRAMMEN AUF SICHERHEITSEIGENSCHAFTEN

(57) Abstract

The invention relates to a method for checking Java byte code programmes for security characteristics. The technical aim of the invention is to provide a method for guaranteeing the best possible security in checking the security characteristics of byte code programmes. According to the invention, the mode of operation of the byte code programme being checked is configured for a finite status transition system (M) and the state space of the JVM is configured for a finite quantity of states in M. After being entered into a model checker, the data of the status transition system (M) is compared with the data in the model checker, the data in the model checker having been entered as a set of conditions (S) for the characteristics of a reliable byte code programme. The byte code programme being checked is only released for further processing if the status transition system (M) fulfils all of the conditions of the set (S). The invention therefore provides a means of guaranteeing the security of byte code programmes and with additional enhancements, can guarantee a certain functionality. This increases the reliability of applications which are run on security–critical platforms such as smart cards.

(57) Zusammenfassung

Die technische Aufgabe ist auf ein Verfahren ausgerichtet, das eine höchstmögliche Sicherheit bei der Überprüfung von Sicherheitseigenschaften von Bytecode–Programmen gewährleistet. Erfindungsgemäß wird die Funktionsweise des zu prüfenden Bytecode–Programms auf ein endliches Zustandsübergangssystem (M) und der Zustandsraum der JVM auf eine endliche Menge von Zuständen in M ausgebildet. Nach Eingabe in einen Modelchecker werden die Daten des endlichen Zustandsübergangssystem (M) mit den im Modelchecker als Bedingungsmenge (S) eingegebenen Daten für Eigenschaften die ein zulässiges Bytecode–Programm kennzeichnen, verglichen. Das zu überprüfende Bytecode–Programm wird nur zur weiteren Verarbeitung freigegeben, wenn das Zustandsübergangssystem (M) alle Bedingungen der Bedingungsmenge (S) erfüllt. Durch die beschriebene Technik kann die Sicherheit von Bytecode–Programmen garantiert und durch zusätzliche Erweiterungen eine gewisse Funktionalität zugesichert werden. Damit kann das Vertrauen in Anwendungen erhöht werden, die auf sicherheitskritischen Plattformen wie Smartcards ablaufen sollen.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Verfahren zur Prüfung von Java-Bytecode-Programmen auf Sicherheitseigenschaften

Beschreibung:

Die Erfindung betrifft ein Verfahren zur Prüfung von Java-Bytecode-Programmen auf Sicherheitseigenschaften nach dem Patentanspruch 1.

Java ist eine von Sun Microsystems entwickelte Programmiersprache, die in sog. Bytecode-Programme übersetzt wird. Obwohl ursprünglich für Java entworfen, eignet sich Bytecode auch als Zielsprache für andere Programmiersprachen, und es gibt bereits entsprechende Compiler (z. B. für Ada).
Das besondere Konzept von Java besteht darin, Programme im Netz abzulegen und von Netzteilnehmern abrufen zu lassen, um sie auf einem Gerät des Netzteilnehmers ablaufen zu lassen. Dies unterstützt z. B. die Konfiguration und Wartung von Geräten aus der Ferne, ist aber auch im Zusammenhang mit Smartcards interessant, deren Funktionalität sich auf diese Weise erweitern läßt. Bytecode-Programme haben folgende Eigenschaften, die für ihren Einsatzzweck bedeutend sind:

- Bytecode-Programme sind kompakt. Bytecode-Instruktionen bieten wesentlich mehr Funktionalität als z. B. Instruktionen von Maschinensprachen. Durch die Anlehnung an Java werden Konzepte wie Objektorientierung direkt unterstützt.
- Bytecode-Programme können effizient interpretiert werden. Dies verleiht solchen Programmen Unabhängigkeit von einer bestimmten Zielmaschine. Vorausgesetzt wird lediglich ein Interpreter (die sog. "Java virtual machine", JVM) auf der Zielmaschine, um beliebige Bytecode-Programme ausführen zu können. Dieser Interpreter kann selbst kompakt implementiert und in (fast) jedes Gerät integriert werden.

Die JVM interpretiert eine Eingabe in Form einer Folge von Zeichen als Bytecode-Programm. Die JVM nimmt dabei keine Prüfungen vor, ob es sich bei der Zeichenfolge tatsächlich um ein Bytecode-Programm handelt. Sie verarbeitet die Zeichen als Bytecode-Befehle, ohne eine genauere Prüfung auf ihre Korrektheit durchzuführen. Die JVM verzichtet auf eine Überprüfung des Bytecodes, da sonst die Ausführungsgeschwindigkeit erheblich leiden würde. Prinzipiell ist es also möglich, eine beliebige Folge von Zeichen als

Bytecode-Programm interpretieren zu lassen. Dadurch wäre es auch möglich - bei genauerer Kenntniss der Implementierung der JVM - ihre Sicherheitsmechanismen zu umgehen und damit z. B. auf dem ausführenden Rechner Daten auszuspähen. Ein sicheres Bytecode-Programm kann dagegen aufgrund des Sprachentwurfs und der JVM auf Daten und Ressourcen des Zielrechners nur zugreifen, indem es dafür Funktionen der JVM in Anspruch nimmt.

Um zu verhindern, daß Zeichenfolgen verarbeitet werden, die keine zulässigen (sicheren) Bytecode-Programme darstellen, ist der JVM ein Prozeß vorgeschaltet, der eine Zeichenfolge auf Konformität zu gewissen Anforderungen überprüft, die sog. Bytecode-Verifikation. Diese Anforderungen garantieren, daß eine Zeichenfolge ein sicheres Bytecode-Programm darstellt. Da diese Überprüfung nur einmal vorgenommen werden muß, entstehen zur Laufzeit keine Nachteile bzgl. der Ausführungsgeschwindigkeit. Der Prozeß der Bytecode-Verifikation prüft eine Folge von Zeichen daraufhin, ob sie ein zulässiges Bytecode-Programm darstellt und damit ohne Gefahr für die Integrität des ausführenden Geräts der JVM zur Interpretierung übergeben werden kann (siehe T. Lindholm, F. Yellin „The Java Virtual Machine Specification"; Sun Microsystems; Addison-Wesley, 1996.

Ein zulässiges Bytecode-Programm ist durch gewisse Eigenschaften gekennzeichnet, die in T. Lindholm, F. Yellin: The Java Virtual Machine Specification. Sun Microsystems, 1996 als "structural constraints" beschrieben werden. Im wesentlichen beschreiben sie die Typsicherheit eines Bytecode-Programms, d. h. in einem Bytecode-Programm sind die Instruktionen so angeordnet, daß eine Instruktion stets solche Daten als Parameter bekommt, die ihrem Typ nach dem entsprechen, was die Instruktion erwartet. Diese Eigenschaften stellen sicher, daß das Bytecode-Programm unter Kontrolle der JVM bleibt und z. B. nicht direkt auf Rechnerressourcen zugreifen kann.

Der Prozeß der Bytecode-Verifikation ist durch zwei Gegebenheiten beschrieben: erstens durch die Beschreibung der Eigenschaften, die er für ein Bytecode-Programm zusichern soll; zweitens durch die Implementierung des Prozesses (dabei handelt es sich um ein C-Programm). Beide Beschreibungen eignen sich nicht, um formale, maschinelle

Berechnungen durchzuführen und damit die Sicherheit von Bytecode-Programmen formal zu garantieren.

Weiterhin ist ein mit Modelchecker bezeichnetes Werkzeug zur Untersuchung von Zustandsübergangssystemen bekannt (siehe K. L. Mc Millan „Symbolic Model Cheking" Kluwer Academic Publishers, 1993).

Zustandsübergangssysteme sind ein allgemeines Modell für Programme, die auf Rechnern oder anderen Maschinen (wie der JVM) ablaufen. Dabei betrachtet man die Zustände, die die Maschine während der Ausführung des Programmes einnimmt und welche Übergänge, d. h. Zustandsänderungen, dabei möglich sind.

Modelchecking ist eine Technik, mit der nur endliche Zustandsübergangssysteme untersucht werden können. Ein Modelchecker untersucht dafür den gesamten Zustandsraum des Systems, um Eigenschaften des Systems zu berechnen. Eine verbreitete Anwendung von Modelcheckern ist, ein System daraufhin zu prüfen, ob es gewisse Eigenschaften erfüllt. Der Modelchecker benötigt dafür als Eingabe eine Beschreibung des Systems, das untersucht werden soll sowie die Beschreibung von Eigenschaften, deren Gültigkeit im System festgestellt werden soll. In beiden Fällen handelt es sich um formale Beschreibungen, d. h. Beschreibungen, deren formale Semantik feststeht, und auf denen somit mathematische Berechnungen durchgeführt werden können.

Im allgemeinen besitzen Software-Systeme auch Bytecode-Programme einen unendlichen Zustandsraum. Das bedeutet, daß das Verfahren des Modelchecking auf Bytecode-programme, die durch einen unendlichen Zustandsraum gekennzeichnet sind, nicht anwendbar ist.

Die technische Aufgabe ist auf ein Verfahren ausgerichtet, das eine höchstmögliche Sicherheit bei der Überprüfung von Sicherheitseigenschaften von Bytecode-Programmen gewährleistet.

Ausgangspunkt des erfindungsgemäßen Verfahrens ist der Sachverhalt, daß ein Bytecode-Programm eine Folge von Zeichen (Bytes) beinhaltet, wobei jedes Zeichen entweder als Instruktion oder als Datum (als Eingabe für die vorhergehende Instruktion) interpretiert wird. Ein Bytecode-Programm stellt somit eine Folge von Instruktionen und zugehörigen

Daten dar. Ein Bytecode-Programm kann damit auch als Beschreibung eines Zustandsübergangssystems gedeutet werden, das Zustände der JVM transformiert. Die Zustände des Systems werden mit den Zuständen der JVM identifiziert und die Übergänge durch die Instruktionen des Programms festgelegt.

Erfindungsgemäß wird das oben beschriebene Zustandsübergangssystem (mit potentiell unendlichem Zustandsraum) durch eine geeignete Abbildung auf ein System mit einer endlichen Anzahl von Zuständen abgebildet. Diese Abstraktion auf eine endliche Anzahl von Zuständen wird dadurch erreicht, daß das System alle Informationen verwirft, die nicht benötigt werden, um festzustellen, ob das ursprüngliche Bytecode-Programm zulässig ist. Dies geschieht im wesentlichen dadurch, daß die konkreten Datenwerte durch reine Typinformationen ersetzt werden. Der Ersatz der konkreten Datenwerte durch reine Typinformationen ist möglich, weil die Zulässigkeit eines Bytecode-Programms nicht von konkreten Werten abhängt. Dabei bleiben aber alle Informationen, die notwendig sind, um die Zulässigkeit des Bytecode-Programms nachzuweisen, erhalten. Das resultierende Zustandsübergangssystem M besitzt eine endliche Menge von Zuständen und erfüllt damit die Grundbedingung für die Bearbeitung in einem Modelchecker. Das resultierende Zustandsübergangssystem M wird in den Modelchecker eingegeben.
In einem weiteren Schritt werden die Eigenschaften, die wie in T. Lindholm, F. Yellin: The Java Virtual Machine Specification. Sun Microsystems, 1996 als "structural constraints" beschrieben, ein zulässiges Bytecode-Programm kennzeichnen, in einer Logik formuliert, die der Modelchecker als Spezifikationssprache für Systemeigenschaften versteht. Das Ergebnis ist eine Menge von Formeln, die dem Modelchecker als Bedingungsmenge S als Vergleichsbasis für das Zustandsübergangssystem M übergeben werden. Aufgrund der o.g. Verfahrensweise ist gewährleistet, daß sich die Formeln nur auf Informationen beziehen, die sowohl im ursprünglichen, potentiell zustandsunendlichen System, als auch im daraus gewonnenen zustandsendlichen System vorhanden sind.

Der Modelchecker wird mit den eben beschriebenen Eingaben gestartet. Als Ergebnis liefert er die Information, ob das Zustandsübergangssystem M die in der Spezifikationssprache als Bedingungsmenge S in Form von Formeln beschriebenen Systemeigenschaften erfüllt. Dabei prüft der Modelchecker für jede Bedingung s der Bedingungsmenge S, ob sie vom

Zustandsübergangssystem M des zu prüfenden Bytecode-Programms erfüllt ist. Wenn das der Fall ist, so ist sichergestellt, daß es sich bei dem ursprünglichen Bytecode-Programm um ein zulässiges Programm handelt, das die Sicherheit des ausführenden Rechners nicht bedroht. Das Bytecode-Programm wird zur weiteren Bearbeitung durch den Rechner freigegeben.

Erfüllen die im Zustandsübergangssystem M erfaßten Daten des zu prüfenden Bytecode-Programms jedoch nicht die in der Bedingungsmenge S in Form von Formeln beschriebenen Systemeigenschaften, die ein Bytecode-Programm kennzeichnen, ist grundsätzlich davon auszugehen, daß das geprüfte Bytecode-Programm die Sicherheit des Rechners bedrohen kann. Das geprüfte Bytecode-Programm wird nicht zur weiteren Bearbeitung freigegeben..

Das erfindungsgemäße Verfahren wird nachfolgend näher erläutert:

Zweck der "Bytecode-Verifikation" ist es, eine Klassendatei, also die Einheit, in der eine Java-Klassenbeschreibung zusammengefaßt ist, auf sichere Ausführbarkeit zu prüfen. Dazu werden die einzelnen Methoden der Klasse (hier Bytecode-Programme genannt) einzeln herausgelöst und der eigentlichen Bytecode-Verifikation unterzogen.

Eine Klassendatei enthält zusätzliche Daten, im wesentlichen Konstanten, auf die in den Bytecode-Programmen Bezug genommen wird. Für die folgenden Schritte ist es vorteilhaft, diese Referenzen in den Bytecode-Programmen aufzulösen und in die Programme einzuarbeiten, bevor mit der eigentlichen Prüfung begonnen wird.

Durch diese Vorverarbeitung erhält man eine Beschreibung der Bytecode-Programme, die sich nicht wesentlich von der ursprünglichen Form unterscheidet.

Die JVM, der Standard-Interpreter für Bytecode-Programme, ist durch eine abstrakte Maschine, d.h. eine Menge von Zuständen, beschrieben. Die Ausführung eines Bytecode-Programms entspricht der Interpretation von Bytecode-Instruktionen durch Zustandsübergänge. Eine Bytecode-Instruktion bewirkt dabei eine Transformation des aktuellen Zustands der JVM in einen neuen Zustand.

Ein Bytecode-Programm definiert also ein Zustandsübergangssystem, wobei der Zustandsraum durch die JVM festgelegt ist und die Übergänge durch die Instruktionen des

Bytecode-Programms bestimmt werden. Dieses Zustandsübergangssystem besitzt einen potentiell unendlichen Zustandsraum. Deshalb ist es nicht geeignet, um von einem Modelchecker untersucht zu werden. Dazu muß es auf ein endliches Zustandsübergangssystem M abgebildet werden. Diese Abbildung wird im folgenden beschrieben.

Es wird nicht zunächst ein unendliches Übergangssystem konstruiert, das anschließend auf ein endliches abgebildet wird. Vielmehr wird aus dem Bytecode-Programm direkt ein endliches Zustandsübergangssystem M konstruiert, unter Verwendung von Regeln, die das Verhalten der Bytecode-Instruktionen beschreiben.

Die Funktionsweise eines Bytecode-Programms wird abgebildet auf ein endliches Zustandsübergangssystem M. Der Zustandsraum der JVM wird auf eine endliche Menge von Zuständen im Zustandsübergangssystem M abgebildet. Die Bytecode-Instruktionen bewirken dann Übergänge auf dieser endlichen Zustandsmenge, wobei ihre prinzipielle Wirkung erhalten bleibt. Das Zustandsübergangssystem M wird so beschrieben, daß diese Beschreibung als Eingabe für den Modelchecker dienen kann.

Die Eingabe für den Modelchecker besteht aus zwei Teilen:

1. Einer als Zustandsübergangssystem M bezeichneten Systembeschreibung, bestehend aus
   - einer Beschreibung des Zustandsraums, festgelegt durch die Zustandsvariablen und ihre Wertebereiche;
   - einer Vorschrift, die die Startzustände des Systems festlegt;
   - einer Übergangsrelation, die angibt, wie Zustände transformiert werden und unter welchen Bedingungen.
2. Einer Menge von Spezifikationen, die als Bedingungsmenge S bezeichnet werden und die die gewünschte Eigenschaften eines zulässigen Bytecode-Programms beschreiben. Diese Eigenschaften werden von dem Zustandsübergangssystem M verlangt, das durch das Bytecode-Programm beschrieben wird. So kann die Sicherheit bei der Ausführung des Bytecode-Programms garantiert werden. Diese Eigenschaften gelten im konkreten, unendlichen Zustandsübergangssystem (und damit im ursprünglichen Bytecode-Programm) dann, wenn sie im abstrakten, endlichen Zustandsübergangssystem M gelten. Der Modelchecker prüft, ob sie im abstrakten Zustandsübergangssystem M

gelten. Falls dies der Fall ist, darf man schließen, daß die Eigenschaften auch vom konkreten System und damit im ursprünglichen Programm erfüllt werden.

Die Erzeugung der erforderlichen Daten wird im folgenden beschrieben:

Der Zustandsraum des Zustandsübergangssystems M ist aus folgenden Komponenten aufgebaut:

- Einem Befehlszähler.
- Einem Operanden-Stack, der die Parameter und Ergebnisse von Instruktionen aufnimmt.
- Einem Feld von lokalen Variablen.
- Einem Feld von globalen Variablen.
- Variablen für das Mitführen von buchhalterischen Informationen; auf diese kann zurückgegriffen werden, um Eigenschaften des Systems zu beschreiben, die mit den übrigen Komponenten nicht beschrieben werden können. Hierzu gehört u.a. ein
- Stack, der Informationen über die aktiven Subroutinen (Unterprogramme in einem Bytecode-Programm) enthält.

Die Werte von Variablen und Stackelementen stammen aus endlichen Wertebereichen. Der Befehlszähler kann eine endliche Zahl von Adresswerten annehmen. Der Operanden-Stack ist in der Höhe begrenzt. Insgesamt ist der Zustandsraum von M dadurch endlich.

Das Befehlsverzeichnis V enthält Beschreibungen aller Bytecode-Instruktionen, bestehend aus folgenden Informationen je Instruktion:

- Die Bezeichnung der Instruktion (1 Byte).
- Die Anzahl der Parameter in Bytes (Zeichen).
- Eine Beschreibung der Wirkung auf Zustände der JVM.
- Bedingungen, die ein Zustand der JVM erfüllen muß, damit die Instruktion angewendet werden kann (C1).
- Bedingungen (C2), die die JVM erfüllen muß, weil die Instruktion im Programm vorkommt. Diese Bedingungen beziehen sich nicht notwendigerweise auf einzelne Zustände, sondern auch auf Ausführungspfade, d.h. Folgen von Zuständen.

Für die Bedingungen in V gilt folgende Eigenschaft (A1): Die Beschreibung der Bedingungen im Befehlsverzeichnis V verwendet nur solche Symbole, die bei der Beschreibung des Zustandsraums für M verwendet werden.

Ein Übersetzer erzeugt aus einem Bytecode-Programm ein endliches Zustandsübergangssystem. Das Bytecode-Programm liegt als Folge von Zeichen in der Eingabe vor, wobei ein einzelnes Zeichen als Instruktion oder Parameter einer Instruktion gedeutet werden kann. Das erste Zeichen wird als Instruktion gedeutet.

Ziel der Übersetzung ist die Konstruktion eines Zustandsübergangssystems M und einer Bedingungsmenge S. Der Übersetzungsprozeß ist wie folgt beschrieben:

1. Beginne mit einem initialen ("leeren") Übergangssystem M. Der Zustandsraum von M ist schon festgelegt durch die abstrakte Repräsentation des JVM-Zustandsraums. Der Startzustand der JVM legt aber den Startzustand von M fest. Es sind jedoch noch keine Übergänge zwischen den Zuständen festgelegt.
2. Beginne mit einer leeren Bedingungsmenge S.
3. Solange Zeichen in der Eingabe vorhanden sind, führe folgende Schritte 4 bis 8 durch:
4. Lies ein Zeichen von der Eingabe; dieses bezeichnet die Programminstruktion B.
5. Schlage im Befehlsverzeichnis V nach, welche Parameter B benötigt.
6. Lies die für B benötigten Parameter P von der Eingabe.
7. Übergebe (B,P) an die Abstraktionskomponente.
8. Übergebe (B,P) an die Bedingungskomponente.

Die Abstraktionskomponente erzeugt aus einer Instruktion B und zugehörigen Parametern P eine Menge von Zustandsübergängen. Das Zustandsübergangssystem M wird um diese Übergänge erweitert.

1. Schlage im Befehlsverzeichnis V nach, welche Wirkung B auf einem Zustand der JVM hat. Die Wirkung ist durch eine Regel beschrieben, so daß sich der Folgezustand der JVM aus einer Berechnung auf dem aktuellen Zustand ergibt. (Eine explizite Angabe der möglichen Übergänge ist nicht möglich, da die JVM über einen (praktisch) unendlichen Zustandsraum verfügt.)
2. Erzeuge daraus eine Beschreibung der Wirkung auf Zustände von M unter Berücksichtigung von P. Die Parameter P gehen in die Berechnung des Folgezustands ein. Wendet man eine JVM-Regel auf einen M-Zustand an, so erhält man eine Menge von M-Zuständen, die die möglichen Folgezustände der JVM repräsentieren. Es ergibt sich eine Menge von Folgezuständen für M, da nicht die konkreten Werte in P, sondern

nur die für M relevanten Informationen betrachtet werden. Welcher JVM-Folgezustand bei Ausführung des Bytecode-Programms tatsächlich eingenommen wird, hängt von den konkreten Werten in P ab.

3. Diese Beschreibung legt eine Menge von Zustandsübergängen fest; erweitere M um diese Übergänge. Diese Übergänge können durch eine Regel beschrieben oder explizit angegeben werden. Letzteres ist möglich, da M nur eine endliche Zahl an Zuständen kennt und deshalb alle Übergänge durch Zustandspaare angegeben werden können. Letztlich lehnt sich die Beschreibung daran an, was der verwendete Modelchecker versteht. Aus praktischen Gründen wird man eine explizite Angabe aller Übergänge vermeiden, da die Datenmenge hierfür weit größer ist als bei der impliziten Angabe durch Regeln.

Die Bedingungskomponente erzeugt aus (B,P) eine Menge von Bedingungen, die vom Modelchecker letztlich zu prüfen sind. Diese Bedingungen können auf verschiedene Art repräsentiert werden, etwa durch temporallogische Formeln.

1. Schlage im Befehlsverzeichnis V nach, welche Bedingungen C1 an den aktuellen JVM-Zustand gestellt werden, damit B ausgeführt werden kann.
2. Übertrage C1 auf entsprechende M-Bedingungen. Laut (A1) sind die Bedingungen in V und die Zustandsbeschreibung für M so aufeinander abgestimmt, daß C1 auf M-Zuständen interpretiert werden kann. Die Übertragung auf M besteht im wesentlichen daraus, mittels P konkrete Instanzen von C1 zu erzeugen und in eine logische Formel zu übersetzen.
3. Schlage entsprechend die Bedingungen C2 nach, die für das gesamte System M durch die Verwendung von B entstehen.
4. Übertrage entsprechend C2 auf M.
5. Erweitere die Bedingungsmenge S um die Darstellungen für C1 und C2.

Die beschriebene Konstruktion des Zustandsübergangssystems M und der Bedingungsmenge S für ein zu prüfendes Bytecode-Programm läuft vollautomatisch ab. Das Befehlsverzeichnis V und seine Bestandteile wird, ebenso wie der Zustandsraum von M, einmal festgelegt für den bestimmten Zweck der "Bytecode-Verifikation", d.h. der Überprüfung von Sicherheitseigenschaften von Bytecode-Programmen.

Nachfolgend wird die Arbeitsweise des Modelcheckers erläutert.

Der Modelchecker prüft für jede Bedingung s aus der Bedingungsmenge S, ob sie vom Zustandsübergangssystem M erfüllt ist. Falls eine Bedingung s nicht erfüllt ist, erzeugt der Modelchecker Informationen, die zusammen mit der Kenntnis, für welche Instruktion s erzeugt wurde, verwendet werden kann, um zu analysieren, wie die Bedingungen an einen sicheren Ablauf der JVM durch das Bytecode-Programm verletzt werden können. Eine typische Ausgabe des Modelcheckers besteht aus der Angabe eines Ausführungspfades, d.h. einer Folge von M-Zuständen, der in einer Verletzung gewisser Bedingungen mündet.

Eine genaue Analyse des Ausführungspfades ist nicht notwendig. Ziel der Bytecode-Verifikation ist es lediglich festzustellen, ob eine Verletzung der Bedingungen durch das Programm möglich ist oder nicht. Informationen über das Wie können interessant sein, sind aber nicht notwendig, da lediglich gefordert ist, potentiell unsichere Programme abzuweisen. Dabei nimmt man in Kauf, auch sichere Programme abzuweisen, die zwar Bedingungen verletzen, deren genauere Analyse aber ergeben würde, daß sie in einer wirklichen Umgebung keinen Schaden anrichten könnten. Da solche Programme i. allg. nicht durch Compiler, sondern nur durch absichtsvolle Codierung entstehen, schränkt man sich nicht wesentlich ein.

Die Steuerung der Bytecode-Verifikation besteht in der Koordinierung der verschiedenen Komponenten. Eine Klassendatei wird der Bytecode-Verifikation unterzogen, indem

1. die Bytecode-Programme (Methoden) einzeln herausgelöst werden,
2. die Referenzen im Bytecode-Programm aufgelöst werden (Vorverarbeitung),
3. ein Zustandssystem und eine Bedingungsmenge konstruiert wird,
4. der Modelchecker mit dieser Eingabe gestartet wird;
5. bei Erfolg des Modelcheckers wird dies für das nächste Bytecode-Programm wiederholt, bei Mißerfolg wird gemeldet, daß die Bytecode-Verifikation für die untersuchte Klassendatei fehlgeschlagen ist.

Das erfindungsgemäße Verfahren läßt sich noch in einigen Punkten erweitern.

Von der Art der Abbildung eines Bytecode-Programms auf ein endliches Zustandssystem hängt es ab, welche Eigenschaften nachgewiesen werden können. Um etwa die Zulässigkeit

eines Bytecode-Programms festzustellen, kann die oben skizzierte Abbildung benutzt werden. Durch Wahl einer anderen Abstraktions-Abbildung ist es möglich, andere Eigenschaften nachzuweisen. Eine interessante Eigenschaft wäre etwa die Beschränkung des Ressourcenverbrauchs eines Bytecode-Programms auf ein gewisses Maß.

Der Einsatz des erfindungsgemäßen Verfahrens erlaubt es, das sicherheitskritische Konzept der Bytecode-Verifikation auf einer formalen Grundlage zu implementieren. Dadurch erreicht man die höchstmögliche Sicherheit für diesen Aspekt der Java-Technologie. Man kann erwarten, daß sich die Technik darüberhinaus auch zum Nachweis weitergehender Eigenschaften von Applets einsetzen läßt, so daß ein größerer Einsatzbereich interessant wird.

Insbesondere im Umfeld Java-fähiger Smartcards (wobei sich Java-fähig darauf bezieht, Bytecode-Programme ausführen zu können), wo die Sicherheitsanforderungen extrem hoch sind, ist diese Technik interessant. Java-fähige Smartcards erlauben es, Programme zu laden und auszuführen, und zwar auch dann, wenn sie sich bereits im Besitz des Endkunden befindet (dies ist mit herkömmlichen Smartcards nicht oder nur eingeschränkt möglich). Dabei ist es von größter Wichtigkeit, daß nur solche Programme geladen und ausgeführt werden, die die Integrität der Karte und der darauf gespeicherten Daten nicht verletzen, denn der Mißbrauch solcher Daten kann erheblichen persönlichen oder finanziellen Schaden anrichten.

Durch die beschriebene Technik kann die Sicherheit von Bytecode-Programmen garantiert und durch zusätzliche Erweiterungen eine gewisse Funktionalität zugesichert werden. Damit kann das Vertrauen in Anwendungen erhöht werden, die auf sicherheitskritischen Plattformen wie Smartcards ablaufen sollen.

Bezugszeichenliste

JVM	Interpreter für Java-Bytecode-Programme (Java Virtual Machine)
M	endliches Zustandsübergangssystem
S	Bedingungsmenge
s	Bedingung von S
V	Befehlsverzeichnis für Bytecode-Instruktionen
C1	Bedingungen, die ein Zustand der JVM erfüllen muß
C2	Bedingungen, die die JVM erfüllen muß
A1	Eigenschaft, die für Bedingungen in V gilt
B	Programminstruktion
P	Parameter für B

Patentansprüche:

1. Verfahren zur Prüfung von Java-Bytecode-Programmen auf Sicherheitseigenschaften nach dem Prinzip der Bytecode-Verifikation,

dadurch gekennzeichnet, daß

a) die Funktionsweise des zu prüfenden Bytecode-Programms unter Verwendung eines Algorithmus, der das Verhalten der Bytecode-Instruktionen beschreibt, von einem potentiell unendlichen Zustandsübergangssystem auf ein endliches Zustandsübergangssystem (M) und der Zustandsraum des Interpreters (JVM) auf eine endliche Menge von Zuständen im endlichen Zustandsübergangssystem (M) abgebildet werden, wobei alle nicht für die Zulässigkeit des zu prüfenden Bytecode-Programms erforderlichen Informationen entfallen, so daß das daraus resultierende endliche Zustandsübergan-gssystem (M) ausschließlich Typinformationen zum Nachweis der Zulässigkeit des Bytecode-Programms enthält, welche in einen Modelchecker eingegeben werden, daß

b) die Eigenschaften, die ein zulässiges Bytecode -Programm kennzeichnen, in einer Logik in Form von Formeln erfaßt und als Bedingungsmenge (S) in den Modelchecker eingegeben werden, wobei der Modelchecker jede einzelne Bedingung (s) der Bedingungsmenge (S) als Spezifikationssprache für Systemeigenschaften von Bytecode-Programmen interpretiert, und daß

der Modelchecker für jede Bedingung (s) der Bedingungsmenge (S) prüft, ob ob sie vom Zustandsübergangssystem (M) erfüllt ist, und daß das überprüfte Bytecode-Programm automatisch zur weiteren Verarbeitung freigegeben wird, wenn das Zustandsübergangssystem (M) alle Bedingungen (s) der Bedingungsmenge (S) erfüllt.

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/EP 99/04438

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 685 792 A (AT&T CORP.) 6 December 1995 (1995-12-06) abstract -----	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 October 1999	28/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Corremans, G

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No
PCT/EP 99/04438

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 685792 A	06-12-1995	CA 2147536 A	02-12-1995
		JP 7334566 A	22-12-1995
		US 5615137 A	25-03-1997

INTERNATIONALER RECHERCHENBERICHT

Intern ales Aktenzeichen
PCT/EP 99/04438

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F11/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 685 792 A (AT&T CORP.) 6. Dezember 1995 (1995-12-06) Zusammenfassung -----	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. Oktober 1999	28/10/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Corremans, G

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internes Aktenzeichen
PCT/EP 99/04438

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 685792 A	06-12-1995	CA 2147536 A	02-12-1995
		JP 7334566 A	22-12-1995
		US 5615137 A	25-03-1997

...F DEM GEBIET DES PATENTWESENS

SC

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
P98033WO.1P			
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*	
PCT/EP 99/04438	25/06/1999	26/06/1998	
Anmelder			
DEUTSCHE TELEKOM AG et al.			

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. _____

   [ ] wie vom Anmelder vorgeschlagen

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

   [X] keine der Abb.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 6 G06F11/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 685 792 A (AT&T CORP.) 6. Dezember 1995 (1995-12-06) Zusammenfassung -----	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. Oktober 1999	28/10/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Corremans, G

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 685792 A	06-12-1995	CA 2147536 A	02-12-1995
		JP 7334566 A	22-12-1995
		US 5615137 A	25-03-1997

T3

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
P98033WO.1P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/04438	25/06/1999	26/06/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK		
G06F11/00		
Anmelder		
DEUTSCHE TELEKOM AG et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.

   ☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

I	☒	Grundlage des Berichts
II	☐	Priorität
III	☐	Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
IV	☐	Mangelnde Einheitlichkeit der Erfindung
V	☒	Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
VI	☐	Bestimmte angeführte Unterlagen
VII	☒	Bestimmte Mängel der internationalen Anmeldung
VIII	☐	Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
10/11/1999	28.04.2000
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:	Bevollmächtigter Bediensteter
Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bozas, I Tel. Nr. +49 89 2399 7408

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/04438

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-12 ursprüngliche Fassung

Patentansprüche, Nr.:

1 ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Es wird auf das folgende Dokument verwiesen:

   D1: EP-A-0 685 792

2. Aufgabe der Erfindung ist es, ein Verfahren zur Prüfung von Java-Bytecode Programmen auf Sicherheitseigenschaften nach dem Prinzip der Bytecode-Verifikation bereitzustellen, mit dem eine höhere Sicherheit bei der Ausführung von solchen Java-Bytecode Programmen gewährleistet wird.

   Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß das Java-Bytecode Programm einem Modelchecker übergeben wird und von letzterem formal geprüft wird, ob das Programm gewisse Sicherheitseigenschaften erfüllt. Um das zu ermöglichen, muß zuerst eine Abbildung des im allgemeinen unendlichen Zustandsraums des Java-Bytecode Programms auf ein anderes geeignetes System mit einer endlichen Anzahl von Zuständen stattfinden, mit dem der Modelchecker arbeiten kann. Dies wird dadurch erreicht, daß alle Informationen, die nicht benötigt werden, um festzustellen, ob das ursprüngliche Bytecode-Programm zulässig ist, verworfen werden. Dies geschieht dadurch, daß die konkreten Datenwerte des Java-Bytecode Programms durch reine Typinformationen ersetzt werden. Das resultierende Zustandsübergangsystem besitzt somit eine endliche Menge von Zuständen and kann von einem Modelchecker bearbeitet werden.

   Der Gegenstand der Erfindung unterscheidet sich von der Lehre des Dokuments D1, dadurch daß die Problematik bezüglich Sicherheit von Java-Bytecode Programmen weder in D1 identifiziert wird noch auf eine mögliche Lösung jener Problematik hingewiesen wird. Obwohl die Lehre des Dokuments D1 zwar die Problematik der formalen Verifikation von Systemen anhand eines Modelcheckers im allgemeinen identifiziert, und einen Algorithmus offenbart, wie man den

Zustandsraum solcher zu verifizierenden Systemen reduzieren kann, wird kein Hinweis gegeben, wie der in D1 beschriebene Algorithmus in dem konkreten Fall auf die Prüfung der Sicherheiteigenschaften von Java-Bytecode Programmen angewendet werden kann. Vor allem, wird kein Hinweis gegeben, daß eine Reduzierung des Zustandsraums des Java-Bytecode Programms durch Ersetzung der konkreten Datenwerte durch reine Typinformationen erzielt werden kann.

Die vorliegende internationale Anmeldung erfüllt somit die Erfordernisse der Artikel 33(2) und (3) PCT hinsichtlich Neuheit und erfinderischer Tätigkeit.

Zu Punkt VII

Bestimmte Mängel der internationalen Anmeldung

1. Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT wurden in der Beschreibung weder der in dem Dokument D1 offenbarte einschlägige Stand der Technik noch dieses Dokument angegeben.

2. Der unabhängiger Anspruch 1 ist zwar in der zweiteiligen Form abgefaßt; alle Merkmale außer "wobei alle nicht für die Zulässigkeit ... welche in einen Modelchecker eingegeben werden" sind aber unrichtigerweise im kennzeichnenden Teil aufgeführt, da sie im Dokument D1 offenbart wurden (Regel 6.3 b) PCT).

3. Folgende Schreibfehler der internationalen Anmeldung sollten korrigiert werden:

   (a) Im Anspruch 1, Zeile 12, sollte "Zustandsübergangssystem" in "Zustandsübergangssystem" korrigiert werden.

   (b) Im Anspruch 1, Zeile 20, sollte "ob ob" in "ob" korrigiert werden.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
P98033WO.1P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 99/04438	25/06/1999	26/06/1998
Anmelder		
DEUTSCHE TELEKOM AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. _____

   [ ] wie vom Anmelder vorgeschlagen

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

   [X] keine der Abb.

EL594609247US

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/04438

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F11/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 685 792 A (AT&T CORP.) 6. Dezember 1995 (1995-12-06) Zusammenfassung -----	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. Oktober 1999	28/10/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Corremans, G

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 99/04438

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 685792 A	06-12-1995	CA 2147536 A	02-12-1995
		JP 7334566 A	22-12-1995
		US 5615137 A	25-03-1997

09/720616

Translation

RECEIVED
SEP 25 2001
Technology Center 2100

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

2

Applicant's or agent's file reference P98033WO.1P	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP99/04438	International filing date (*day/month/year*) 25 June 1999 (25.06.99)	Priority date (*day/month/year*) 26 June 1998 (26.06.98)
International Patent Classification (IPC) or national classification and IPC G06F 11/00		
Applicant DEUTSCHE TELEKOM AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 November 1999 (10.11.99)	28 April 2000 (28.04.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP99/04438

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-12, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. 1, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____,
Nos. _____, filed with the letter of _____.

☐ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1	YES
	Claims		NO
Inventive step (IS)	Claims	1	YES
	Claims		NO
Industrial applicability (IA)	Claims	1	YES
	Claims		NO

2. Citations and explanations

1. This report makes reference to the following document:

D1: EP-A-0 685 792.

2. The problem addressed by the invention is that of providing a method for checking Java byte code programs for security characteristics according to the principle of byte code verification with which higher security is ensured when Java byte code programs of this type are used.

This problem is solved according to the invention in that the Java byte code program is supplied to a model checker which formally checks whether the program fulfills certain security characteristics. In order for this to be possible, the generally infinite state space of the Java byte code program must first be imaged in another suitable system with a finite number of states with which the model checker can function. This is achieved by discarding all information which is not necessary for determining whether the original byte code program is acceptable. This takes place in that the concrete data values of

the Java byte code program are replaced by pure model information. The resulting status transition system thus has a finite amount of states and is compatible with a model checker.

The subject matter of the invention differs from the teaching of D1 in that the problem of security of Java byte code programs is not identified in D1 and that document does not suggest a possible solution to the specified problem. Although the teaching of D1 identifies, in general, the problem of formal verification of systems using a model checker and discloses an algorithm as to how the state space of these systems to be verified can be reduced, there is no mention of how the algorithm described in D1 can be used to check security characteristics of Java byte code programs. Most importantly, it is not suggested that the state space of the Java byte code program can be reduced by replacing the concrete data values by pure model information.

The present international application therefore meets the requirements of PCT Article 33(2) and (3) with regard to novelty and inventive step.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to PCT Rule 5.1(a)(ii), the description does not cite D1 or indicate the relevant prior art disclosed therein.

2. Independent Claim 1 has been drafted in the two-part form; all features except for "all the information which is not necessary for accepting ... which is entered into a model checker" are, however, incorrectly included in the characterizing part, since they were already disclosed in D1 (PCT Rule 6.3(b)).

3. The following typing errors in [the German text of] the international application should be corrected:

   (a) The hyphen should be deleted from the word written as "Zustandsübergan-gssystem" in Claim 1, line 12.

   (b) In Claim 1, line 20, "ob ob" should be corrected to "ob".